Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
628 East 9th Street
Houston TX 77007-1722
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson
fjohnson@azalaw.com (SBN 289055)
Joseph Ahmad (*pro hac vice forthcoming*)
jahmad@azalaw.com
Nathan Campbell (*pro hac vice forthcoming*)
ncampbell@azalaw.com
AHMAD, ZAVITSANOS, & MENSING, PLLC
1221 McKinney Street, Suite 3460
Houston TX 77010
Tel: (713) 655-1101
Fax: (713) 655-0062

Attorneys for Plaintiff

[Additional Counsel included on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of others similarly situated, *Plaintiff*, *v.* THE COUNTY OF SANTA CLARA d/b/a SANTA CLARA VALLEY MEDICAL CENTER *Defendant*.	CASE NO. **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL** Filed August 25, 2023

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all other current California citizens similarly situated, brings suit against Defendant the County of Santa Clara d/b/a Santa

Clara Valley Medical Center ("Defendant" or "Santa Clara Valley Medical Center"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

I. SUMMARY OF ALLEGATIONS

1. This case arises from Defendant's systematic violation of the medical privacy rights of patients and users of Defendant's services, exposing highly sensitive personal information to Facebook without those patients' or users' knowledge or consent.

2. At all relevant times, Defendant disclosed information about prospective and actual patients—including their status as actual or potential patients, their actual or potential physicians, their actual or potential medical treatments, the hospitals they visited or may visit, and their personal identities—to Facebook, Google, and other third parties without their prospective or actual patients' knowledge, authorization, or consent.

3. Defendant disclosed this protected health information through the deployment of various digital marketing and automatic software tools embedded in its website and patient portal that purposefully and intentionally disclose Personal Health Information to Facebook, Google, and other third parties who exploit that information for advertising purposes. Defendant's use of these tools caused personally identifiable information and the contents of communications exchanged between actual and prospective patients with Defendant to be automatically redirected to Facebook, Google, and other third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, and their rights as citizens of California.

4. Defendant's conduct in disclosing such protected health information to Facebook violates California law, including the California Invasion of Privacy Act ("CIPA"), CAL. PENAL CODE §§ 630, et seq.; the California Confidentiality of Medical Information Act ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101; and the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), CAL. PENAL CODE § 502.

5. Plaintiff continues to desire to search for health information on Defendant's websites as it is often her only means to seek and facilitate treatment. Plaintiff will continue to suffer harm if the websites are not redesigned. If the websites were redesigned to comply with applicable laws, Plaintiff would use Defendant's websites to search for health information in the future.

6. On behalf of herself and all similarly situated current Citizens of California, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of personal information; awarding statutory damages as allowed under law; actual damages; attorney's fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

II. PARTIES

A. Plaintiff

7. Plaintiff Jane Doe is a resident of Santa Clara County, California.

8. Plaintiff Jane Doe has used Defendant's website and patient portal to search for doctors and medical treatment and to manage her treatment.

9. Plaintiff Jane Doe's use of the Defendant's website entailed providing her sensitive medical information, such as conditions for which she was seeking treatment.

B. Defendant

10. Defendant County of Santa Clara is the managing agent for Santa Clara Valley Medical Center, which has its principal place of business at 751 S. Bascom Avenue, San Jose, CA 95128. Santa Clara Valley Medical Center operates multiple hospitals and clinics, including Santa Clara Valley Medical Center, O'Connor Hospital, St. Louise Regional Hospital, Valley Health Center San Jose, Valley Health Center Sunnyvale, Valley Health Center Gilroy, and Valley Health Center Milpitas.[1] Defendant also owns and operates both a website and patient portal for its patients, which can be accessed at https://scvmc.scvh.org/home.

[1] https://scvmc.scvh.org/home

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 putative class members, and at least one Class Member is a citizen of a different state from Defendant.

12. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout California, including in Santa Clara County, and has its principal place of business in California.

13. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this district and because a substantial portion of the events and omissions giving rise to the claims occurred in this District.

IV. COMPLIANCE WITH THE GOVERNMENT TORT CLAIMS ACT

14. Prior to filing this complaint, Plaintiff complied with the government tort claims process set forth in Cal. Gov. Code §§ 810-996.6, et seq.

15. On June 20, 2023, Plaintiff filed a written claim for damages against Defendant County of Santa Clara, asserting the privacy claims that are the subject of this lawsuit.

16. On August 4, 2023, counsel for Defendant County of Santa Clara provided a Notice of Rejection of Claim letter to Plaintiff rejecting Plaintiff's claims.

V. FACTUAL BACKGROUND

17. Defendant's website and patient portal allows patients like Plaintiff to facilitate all aspects of their care with Defendant, allowing them to find doctors, research treatments, access medical records, pay bills, access its patient portal, view lab results, and refill prescriptions. Since 2018, Plaintiff has used Defendant's website and patient portal (Defendant's "Web Properties") for those purposes.

18. Plaintiff is a longtime Facebook user, who has had an account with Facebook since 2009.

19. Plaintiff has been a patient of Santa Clara Valley Medical Center since 2017. Plaintiff has regularly visited Defendant's website and patient portal since 2018 at https://scvmc.scvh.org. She used Defendant's website typically once a month to search for treatments for her conditions, including cirrhosis of liver and ascites, generalized anxiety disorder, migraines, and carpal tunnel syndrome. That research revealed treatments and tests for those conditions and others, including psychiatric treatment, physical therapy, and pain management. It also allowed her to access her lab results, schedule doctor's appointments, refill prescriptions, and communicate with her doctors. To do so, she needed to disclose her health information, something she did while trusting that Defendant would only use it to facilitate her care.

20. Plaintiff has used Defendant's website to make appointments with a gynecologist for treatment related to endometriosis, pelvic floor disorder, and menopause.

21. Plaintiff has also used Defendant's website to make appointments with a psychologist for treatment related to post-traumatic stress disorder, panic attacks, and a personality disorder.

22. Plaintiff has also used Defendant's website to order medications for women's health issues, including endometriosis, as well as for pancreatitis, asthma, fibromyalgia, and pain management.

23. Between January 1, 2023 and June 30, 2023, Plaintiff used Defendant's website to view test results regarding testing for undiagnosed seizures, as well as bone density scans, scans related to arthritis, an endoscopy, an ultrasound of her liver, and an MRI of her brain.

24. In June 2023, Plaintiff used the "Find a Provider" function on Defendant's website to locate a neurologist.

25. Unbeknownst to Plaintiff Jane Doe, Defendant had embedded source code on its website that took every search term she entered and every page of the site she visited and sent that information directly to Facebook, the largest and most profitable social media company on the planet. Defendant accomplished this by installing Facebook's "Meta Pixel" tool on almost every

page of Defendant's website. The Meta Pixel worked like a listening device. Each time Plaintiff Jane Doe typed a search term, the Meta Pixel recorded the information she entered and transmitted it to Facebook, along with identifying information that let Facebook know exactly who Jane Doe was. Instantaneously, Facebook knew the conditions for which Plaintiff was seeking medical treatment.

26. Facebook then took this information and added it to all of the other information it keeps about consumers, matching Plaintiff's interest in medical care with her Facebook profile, name, address, interests, and other websites he had visited. This information then became available for Facebook's advertisers to use when Facebook sold them targeted advertising services.

27. After using Defendant's patient portal, Plaintiff saw numerous advertisements in her Facebook feed for products and services related to the medical conditions for which she had entered data inside the patient portal, including advertisements for pain management. These advertisements included advertisements for medications for her various conditions, as well as solicitations to participate in research questionnaires, research studies, and clinical trials.

28. Plaintiff was surprised and troubled that information she believed she was communicating only to Defendant for the purpose of obtaining medical treatment had been sent to Facebook, Google, and other third parties. Plaintiff subsequently learned that thousands of Defendant's patients had similarly had their privacy rights violated. Most of these patients were likely not even aware of this privacy violation, much less able to hire counsel to stop the illegal conduct. Plaintiff therefore now brings these claims to correct Defendant's privacy violations and obtain relief for herself and thousands of similarly situated patients.

VI. CLASS ACTION ALLEGATIONS

A. Defendant routinely disclosed the protected health information of patients and users of their services to Facebook.

29. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending

life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

30. Medical patients and those seeking medical treatment in California such as Plaintiff have a legal interest in preserving the confidentiality of their communications with health care providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

31. As a health care provider, Defendant has common law and statutory duties to keep patient data, communications, diagnoses, and treatment information completely confidential unless authorized to make disclosures by the patient.

32. Patients are aware of (and must be able to rely upon) the protections, obligations, and expectations provided by statutory, regulatory, and common law as well as the promises of confidentiality contained within the Hippocratic Oath.

33. Defendant operates websites for current and prospective patients, including https://scvmc.scvh.org.

34. Defendant's Web Properties are designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues and treatment options, and joining support groups.

35. Defendant encourages patients to use digital tools on its websites to seek and receive health care services.

36. The home page of Defendant's website is designed for use by patients. The homepage provides patients with tools to seek medical treatment, such as finding a doctor, researching services and treatments, and paying bills.

37. Defendant also maintains a patient portal, which allows patients to make appointments, access medical records, view lab results, and exchange communications with health

care providers. Source code on Defendant's website causes these communications to be intercepted and disclosed to multiple third parties, including Google.

38. Defendant encourages patients to use digital tools on its websites to seek and receive health care services. Plaintiff and Class Members provided their private information to Defendant's website with the reasonable understanding that Defendant would secure and preserve the confidentiality of that information.

39. Plaintiff and Class Members exchanged numerous communications with Defendant. Plaintiff's and Class Members' communications included logging in and out of patient portals, exchanging communications about doctors and health conditions, and using button functionality from defendant's websites.

40. Notwithstanding prospective and current patients' reasonable expectations of privacy and Defendant's legal duties of confidentiality Defendant disclosed (and continues to disclose) the contents of Plaintiff's and Class Members' communications and protected health information via automatic mechanisms embedded in the websites operated by Defendant without patients' knowledge, authorization, or consent. In doing so, Defendant systematically violated the medical privacy rights of Plaintiff and Class Members by causing the unauthorized disclosure of their communications to be transmitted to Facebook, Google, and other third-party marketing companies.

41. The private information provided by Plaintiff and Class Members has been—and likely will be—further disseminated to additional third parties.

42. While Defendant intentionally incorporated the Meta Pixel into its website, Defendant never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications with Facebook. As a result, Plaintiff and Class Members were unaware that their private information was being surreptitiously transmitted to third parties, including Facebook and Google, when they visited Defendant's website.

43. By design, none of the tracking mechanisms employed by Defendant are visible to patients visiting Defendant's website.

44. Defendant did not warn or otherwise disclose to Plaintiff and Class Members that Defendant bartered their confidential medical communications to Facebook, Google, and other third parties for marketing purposes.

45. Plaintiff and Class Members never consented, agreed, or otherwise authorized Defendant to disclose their confidential medical communications.

46. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as patients;

b. Plaintiff's and Class Members' communications with Defendant via its website;

c. Plaintiff's and Class Members' use of Defendant's patient portal;

d. Plaintiff's and Class Members' searches for information regarding specific medical conditions and treatments, their medical providers, and their physical location.

47. Defendant interfered with Plaintiff's and Class Members' privacy rights when it implemented technology that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential information to Facebook, Google, and other third parties.

48. Defendant also breached its obligations to patients in multiple other ways, including (1) failing to obtain their consent to disclose their private information to Facebook and other third parties, (2) failing to adequately review its marketing programs and web-based technology to ensure its website was safe and secure, (3) failing to remove or disengage software code that was known and designed to share patients' private information with third parties, (4) failing to take steps to block the transmission of Plaintiff's and Class Members' private information to Facebook and other third-party advertising companies, (5) failing to warn Plaintiff and Class Members that Defendant was routinely bartering their private information to Facebook

via the Meta Pixel, and (6) otherwise ignoring Defendant's common-law and statutory obligations to protect the confidentiality of patient's protected health information.

49. Plaintiff and Class Members have suffered injury because of Defendant's conduct. Their injuries include invasion of privacy and the continued and ongoing risk of irreparable harm from the disclosure of their most sensitive and personal information.

B. The Nature of Defendant's Unauthorized Disclosure of Patients' Health Care Information

50. Defendant's disclosure of current and prospective patients' personal health information occurs because Defendant intentionally deploys source code on the websites it operates, which causes current and prospective patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

51. By design, third parties receive and record the exact contents of these communications before the full response from Defendant has been rendered on the screen of the patient's or user's computer device and while the communication with Defendant remains ongoing.

52. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, not just the name of a physician and field of medicine, but also the first name, the last name, email address, phone number and zip code and city of residence entered into the booking form. In addition, that data is linked to a specific internet protocol ("IP") address.

53. The Meta Pixel, for example, sends information to Facebook via scripts running in a person's internet browser so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.

54. In addition, if the person is (or recently has) logged into Facebook when they visit a particular website when a Meta Pixel is installed, some browsers will attach third-party cookies—another tracking mechanism—that allow Meta to link pixel data to specific Facebook accounts.

55. The Meta Pixel allows Facebook to track people and the actions they take on websites. When Meta Pixel is installed on a hospital website or patient portal like those maintained by Defendant, the information that Facebook receives may include such information as the patient's home address, their name, their search location, as well as their doctor's specialty, name, and gender. When combined with other information that Facebook receives via the Meta Pixel (such as Plaintiff's appointment information and information about the kinds of treatments that patients research on the hospital's website), Facebook learns about patients' past and future medical conditions, their past and future medical treatment, and when and where they are receiving treatment for those conditions.

56. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Personal Health Information, like Facebook, implement workarounds that cannot be evaded by savvy users. Facebook's workaround, for example, is called Conversions API (CAPI).

57. CAPI is an effective workaround because it does not intercept data communicated from the user's browser. Instead, Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

58. Thus, the communications between patients and Defendant, which are necessary to use Defendant's website, are actually received by Defendant and stored on its server before CAPI collects and sends the Personal Health Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

59. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct companies to use the CAPI in addition to the Pixel and share the same events using both tools because such a redundant event setup allows website owners to share website events with Facebook that the pixel may lose. Thus, it is reasonable to infer that Facebook's customers who

implement the Meta Pixel in accordance with Facebook's documentation will also implement the CAPI workaround.

60. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

61. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer a user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

62. For example, when Plaintiff or a Class Member accessed Defendant's website pages hosting the Meta Pixel, the Meta Pixel software directed their browsers to send a message to Facebook's servers. The information that Defendant sent to Facebook included the private information that Plaintiff and Class Members communicated to Defendant's website, such as the type of medical appointment the patient made, the date, and the specific doctor the patient was seeing. Such private information allows third-party advertising companies like Facebook to determine that a specific patient was seeking a specific type of confidential medical treatment. This kind of disclosure also allows Facebook to reasonably infer that a specific patient was being treated for specific types of medical conditions, such as cancer.

63. Websites like those maintained by Defendant are hosted by a computer server through which the businesses in charge of the website exchange and communicate with internet users via their web browsers.

64. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with internet users via a client device, such as a computer, tablet, or smart phone, via the client device's web browser.

65. Web browsers are software applications that allow users to exchange electronic communications over the internet.

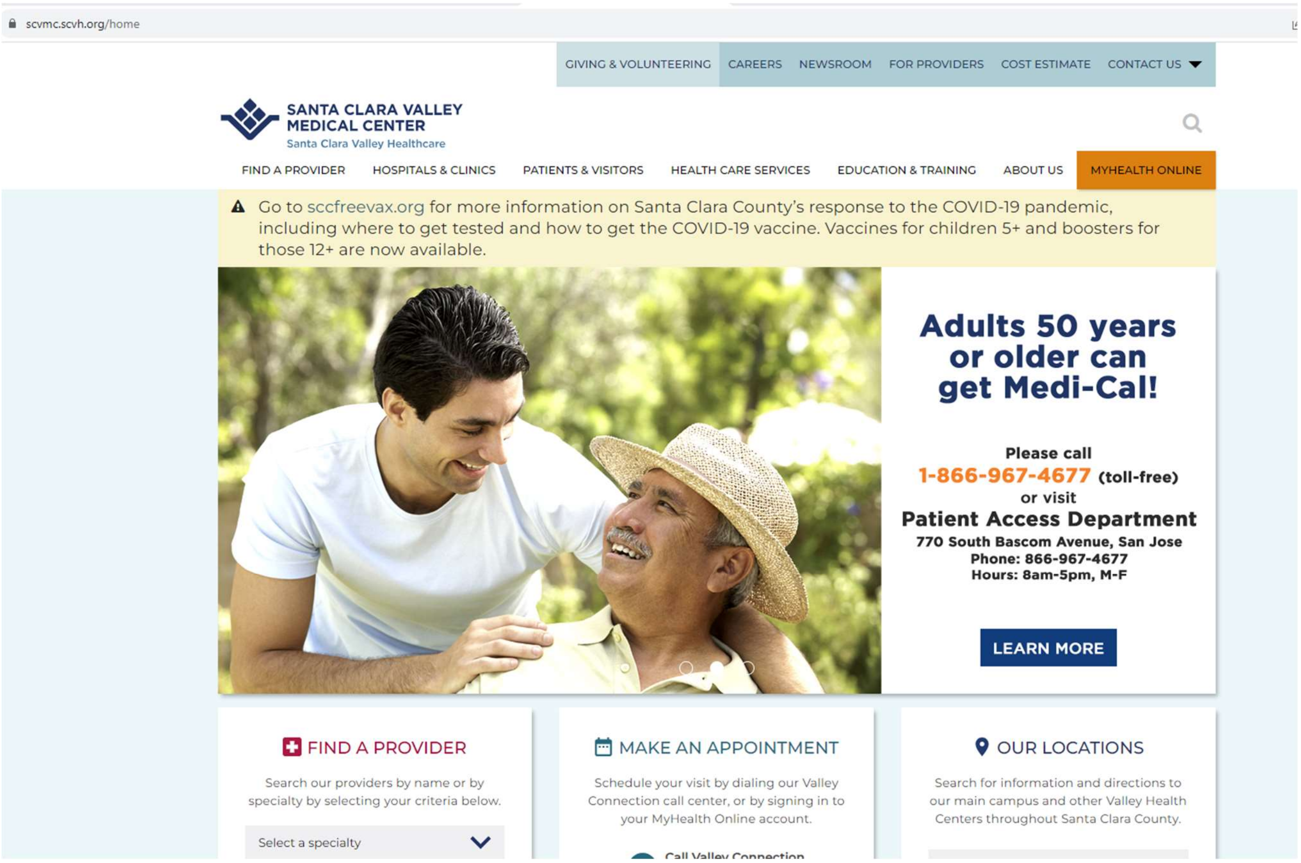
66. Each exchange of an electronic communication over the internet consists of an HTTP request from a client device and an HTTP response from a server. When a user types a URL into a web browser, for example, the URL is sent as an HTTP request to the server corresponding to the web address, and the server then returns an HTTP response that consists of a web page to render in the client device's web browser.

67. In addition to specifying the URL, HTTP requests can also send data to the host server, including users' cookies. Cookies are text files stored on client devices to record data, often containing sensitive, personally identifiable information.

68. In turn, HTTP responses may consist, among other things, of a web page, another kind of file, text information, or error codes.

69. A web page consists primarily of "Markup" and "Source Code." The markup of a web page comprises the visible portion of that web page. Markup is displayed by a web browser in the form of words, paragraphs, images, and videos displayed on a users' device screen. The source code of a web page is a set of instructions that commands the browser to take certain actions, either when the web page loads or when a specified event triggers the code.

70. For example, typing https://scvmc.scvh.org/home into a web browser sends an http request to Defendant's website, which returns a HTTP response in the form of the home page of Defendant's website:



Go to sccfreevax.org for more information on Santa Clara County's response to the COVID-19 pandemic, including where to get tested and how to get the COVID-19 vaccine. Vaccines for children 5+ and boosters for those 12+ are now available.

Adults 50 years or older can get Medi-Cal!

Please call
1-866-967-4677 (toll-free)
or visit
Patient Access Department
770 South Bascom Avenue, San Jose
Phone: 866-967-4677
Hours: 8am-5pm, M-F

FIND A PROVIDER

Search our providers by name or by specialty by selecting your criteria below.

MAKE AN APPOINTMENT

Schedule your visit by dialing our Valley Connection call center, or by signing in to your MyHealth Online account.

OUR LOCATIONS

Search for information and directions to our main campus and other Valley Health Centers throughout Santa Clara County.

71. Source code is not visible on the client device's screen, but it may change the markup of a webpage, thereby changing what is displayed on the client device's screen. Source code may also execute a host of other programmatic instructions, including commanding a web browser to send data transmissions in the form of HTTP requests to the website's server, or, as is the case with Defendant's website, to third parties via pixels.

72. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,[2] effectively opening a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties, along with patients' personally identifiable information like their Facebook IDs.

[2] These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

73. For example, Defendant's website includes software code that transmits HTTP requests *directly* to Facebook, including patients' private health information, every time a patient interacts with a page on its website.

74. In essence, Defendant encourages its patients to use a tapped device, and once the Webpage is loaded into a patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties, including Facebook and Google.

75. When a patient communicates with Defendant's website (whether by typing in a webpage, putting in a search, clicking on a hyperlink, logging into the Defendant patient portal, maneuvering through the patient portal, or otherwise), Defendant causes some of that information to be transmitted to third parties without the patient's knowledge or authorization. The third parties to whom user data is transmitted and the content of communications redirected are typically procured by websites to track users' personally identifiable data and communications for marketing purposes—i.e., targeted advertising.

76. The basic command that web browsers use to exchange data and user communications is called a GET request.[3] For example, when a patient types "heart failure treatment" into the search box on Defendant's website and hits 'Enter,' the patient's web browser makes a connection with the server for Defendant's website and sends the following request: "GET search/q=heart+failure+treatment."

77. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

[3] https://www.w3schools.com/tags/ref_httpmethods.asp

78. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications, in this case Defendant's server, will send a set of instructions to the web-browser, commanding the browser with source code that (1) directs the browser on how to render the entity's response and, in many circumstances, (2) commands the browser to transmit personally identifiable data about the Internet user and re-direct the precise content of the user's GET or POST requests to various third parties.

79. Unbeknownst to most users, however, the website's server may also transmit the user's communications to third parties. For example, the Meta Pixel that Defendant installed on its website is programmed to manipulate user's browsers so that their communications with Defendant were automatically, contemporaneously, and surreptitiously sent to Facebook. When Plaintiff and Class Members visited Defendant's website for the first time, the Meta Pixel source code that Defendant had installed on its website instructed Plaintiff's and Class Members' browsers to begin sending duplicate GET and POST requests to Facebook every time that Plaintiff and Class Members subsequently interacted with part of Defendant's website, such as browsing new pages, filling out forms, or entering search terms in a search box.

80. The Meta Pixel was triggered each time Plaintiff and Class Members communicated with Defendant via Defendant's website and patient portal. This resulted in Plaintiff's and Class Members' communications being intercepted, duplicated, and secretly transmitted to Facebook at the same time the communications (in the form of HTTP GET requests and HTTP POST requests) were transmitted to Defendant.

81. In other words, as a result of the source code that Defendant installed on its website, *two* communications originate from a patient's browser once the patient initiates an action on Defendant's website—one (as intended) sent to Defendant and a second (undetectable to patients like Plaintiff and Class Members) that was simultaneously sent to Facebook. Accordingly, at the same time Plaintiff's and Class Members' browsers sent communications to

Defendant, a duplicate of those communications was simultaneously sent to Facebook as a result of the instructions that their browsers had previously received from Defendant's website.

82. Given that the two communications are literally generated and sent at the same time, the duplication is occurring while the intended communications are in transit. Effectively, it is as if Defendant planted a bugging device inside Plaintiff's and Class Members' telephones, so that when they placed a call, the bug simultaneously sent a radio signal to Facebook in the next room, allowing Facebook to listen in and record the call. In this way, Defendant aided Facebook to read, learn, and exploit the contents of Plaintiff's and Class Members' communications that they sent (and Defendant received) within the state of California.

83. Google warns website developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.[4]

84. Worse, the Personal Health Information that Defendant's Meta Pixel sent to Facebook was sent alongside Plaintiff's and Class Members' Facebook IDs (c_user cookie or "FID") thereby allowing individual patients' communications with Defendant, and the Personal Health Information contained in those communications, to be linked to their unique Facebook accounts.

85. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

86. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

[4] https://support.google.com/platformspolicy/answer/6156630?hl=en

87. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

88. Web bugs can be placed directly on a page by a web developer or can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom the website transmits personally identifiable user data and re-directs the content of communications.

89. On information and belief, Defendant deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the Defendant's Web Properties, including inside Defendant's patient portal, that is, in reality, an invisible window through which Defendant funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

90. By design, none of the tracking is visible to patients who visit Defendant's Web Properties.

91. Once the initial connection is made between a user and a website, the communications commence and continue between the parties in a bilateral fashion until the user leaves the website.

92. Unbeknownst to most users, the website's server may also transmit the user's communications to third parties. Indeed, Google warns website developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.[5]

93. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

[5] https://support.google.com/platformspolicy/answer/6156630?hl=en

94. These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

95. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must include the third-party source code directly in their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

96. More significantly, tracking pixels such as the Meta Pixel tool allow Defendant and Facebook to secretly track, intercept, record, and transmit every patient communication made on Defendant's website. When patients visit Defendant's website, unbeknownst to them, the web page displayed on the patient's browser includes the Meta Pixel as embedded code, which is not visible to patients or other visitors to Defendant's website. This code is triggered when a patient or visitor interacts with the web page. Each time the Meta Pixel is triggered, the software code is executed and sends patient's private information directly to Facebook.

97. The Meta Pixel and similar tracking pixels act like a physical wiretap on a phone. Like a physical wiretap, pixels do not appear to alter the function of the communication device on which they are surreptitiously installed. Instead, these pixels lie in wait until they are triggered by an event, at which time they effectively open a channel through the website that funnels data about users and their actions to third parties via a hidden HTTP request that is never shown to or agreed to by the user.

98. For example, a patient can trigger an HTTP request by interacting with the search bar on Defendant's website by typing a term such as "pregnancy" into the search bar and then hitting enter. Defendant's server in turn sends an HTTP response, which results in the search results being displayed.

99. This is not the only HTTP request, however, that is created by a patient's interaction with Defendant's website. In fact, at the very same time the web page is instructed to

send an HTTP request to Defendant requesting search results, the source code, acting as a tap, is triggered, such that Defendant's website is also instructed to send an HTTP request directly to Facebook, Google, and other third parties, informing them of the patient's exact search and the patient's identifiable information.

C. Tracking pixels provide third parties with a trove of personally identifiable information.

100. Tracking pixels are especially pernicious because they result in the disclosure of personally identifiable information.

101. For example, an IP address is a number that identifies a computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.[6]

102. Because of their uniquely identifying character, IP addresses are considered protected personally identifiable information. 45 CFR § 164.514. Tracking pixels can (and typically do) collect website visitors' IP addresses.

103. HIPAA further provides that information is personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

104. Consequently, Defendant's disclosure of Plaintiff's and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

105. Likewise, internet cookies also provide personally identifiable information.

106. In the early years of the internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports

[6] https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

section of a traditional newspaper, advertisers on the early internet paid for ads to be placed on specific web pages based on the type of content displayed.

107. Computer programmers eventually developed 'cookies'—small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Eventually some cookies were designed to acquire and record an individual internet user's communications and activities on websites across the internet.

108. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers.

109. Cookies are considered personal identifiers. 45 CFR § 164.514. Tracking pixels can collect cookies from website visitors.

110. In general, cookies are categorized by (1) duration and (2) party.

111. There are two types of cookies classified by duration.

112. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

113. "Persistent cookies" are designed to survive beyond a single internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's internet communications for years and over dozens or even hundreds of websites. Persistent cookies are also called "tracking cookies."

114. Cookies are also classified by the party that uses the collected data.

115. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. First-party cookies can be helpful to the user, server, and/or website to assist with security, login, and functionality.

116. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits Defendant's website will also have cookies on their device from third parties, such as Facebook and Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

117. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to a user's communications and habits. To build individual profiles of internet users, third party data companies assign each user a unique identifier or set of unique identifiers.

118. Traditionally, first-party and third-party cookies were kept separate. An internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Defendant can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record a patient's communications, Defendant is not permitted direct access to Facebook third-party cookie values. The reverse *was* also true: Facebook was not provided direct access to the values associated with first-party cookies set by companies like Defendant. But Data companies have designed a way to hack around the same-origin policy so that third-party data companies like Facebook can gain access to first-party cookies.

119. JavaScript source code developed by third party data companies and placed on a webpage by a developer such as Defendant can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as

"cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information that they have collected and recorded about a user that is associated with a cookie identifier number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

120. In effect, cookie synching is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set for first-party websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking.

121. The Facebook cookie used for cookie synching is named _fbp.

122. On information and belief, the letters fbp are an acronym for Facebook Pixel.

123. The Facebook _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the health care provider using the Meta Pixel.

124. The _fbp cookie is also a third-party cookie in that it is also a cookie associated with Facebook that is used by Facebook to associate information about a person and their communications with non-Facebook entities while the person is on a non-Facebook website or app.

125. Defendant requires patients using its patient portal to have enabled first-party cookies to gain access to its patient portal.

126. The _fbp cookie is used as a unique identifier for patients by Facebook.

127. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Facebook cookie—because Facebook has disguised it as a first-party cookie. Facebook also uses IP addresses and user-agent information to match the health information it receives from Defendant with Facebook users.

128. Defendant engages in cookie synching with Facebook, Google, and other third parties.

129. Defendant's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Defendant assigns to patients to also be made to third parties.

130. Defendant uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

131. A third type of personally identifiable information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

132. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[7] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[8] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[9]

133. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[10]

[7] https://www.blog.google/products/chrome/building-a-more-private-web/

[8] https://pixelprivacy.com/resources/browser-fingerprinting/

[9] https://www.blog.google/products/chrome/building-a-more-private-web/

[10] https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

134. Browser-fingerprints are personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

135. Defendant uses and causes the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

136. A fourth kind of personally identifiable information protected by law against disclosure are unique user identifiers (such as Facebook's "Facebook ID") that permit companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is an identifying number string that is connected to a user's Facebook profile.[11] Anyone with access to a user's Facebook ID can locate a user's Facebook profile.[12]

137. Unique identifiers such as a person's Facebook ID are likewise capable of collection through pixel trackers.

138. Each of the individual data elements described above is personally identifiable on their own. However, Defendant's disclosures of such personally identifiable data elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies such as Facebook, Google, and other internet marketing companies that expressly state that they use such data elements to identify individuals.

D. Facebook's Business Model: Exploiting Users' Personal Information for Profit

139. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

[11] https://www.facebook.com/help/211813265517027

[12] https://smallseotools.com/find-facebook-id/

140. Facebook describes itself as a "real identity" platform.[13] This means that users are permitted only one account and must share "the name they go by in everyday life."[14] To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.[15]

141. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."[16] Facebook has since evolved into one of the largest advertising companies in the world.[17] Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.[18] This allows Facebook to make inferences about users based on their interests, behavior, and connections.[19]

142. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.[20]

143. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code.

[13] https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.

[14] https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/

[15] https://www.facebook.com/help/406644739431633

[16] https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

[17] https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

[18] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[19] https://www.facebook.com/business/ads/ad-targeting

[20] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

144. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

145. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[21] Aided by highly granular data used to target specific users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

146. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

147. One of Facebook's most powerful tools is called the "Meta Pixel."

[21] https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

148. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website.[22] Once activated, the Meta Pixel "tracks the people and type of actions they take."[23] Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.[24] The Meta Pixel code works by sending Facebook a detailed log of a user's interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website or how far down a web page they scrolled.[25]

149. When a patient uses their healthcare provider's website or application where the Meta Pixel is present, the Meta Pixel transmits the content of their communications to Facebook, including but not limited to (1) signing up for a patient portal, (2) signing-in and -out of a patient portal, (3) taking actions inside a patient portal, (4) making or scheduling appointments, (5) exchanging communications related to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions, (6) conduct a search on a Facebook partner website, and (7) other information that qualifies as Personal Health Information and/or Protected Health Information under state and federal laws.

150. In many circumstances, Facebook also obtains information from health care providers that identify a Facebook user's status as a patient and other health information that is protected by state and federal law. This occurs through tools that Facebook encourages health care providers to use to upload customer (i.e., patient) lists for use in its advertising systems.

151. The information transmitted from a health care provider's website or application is sufficient to uniquely identify a patient under federal law (such as IP addresses and device

[22] https://developers.facebook.com/docs/meta-pixel/

[23] https://www.facebook.com/business/goals/retargeting

[24] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[25] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

identifiers that Facebook associates with a patient's Facebook account), and may also include a patient's demographic information, email address, phone number, computer IP address, contact information, appointment type and date, treating physicians, button and menu selections, the content of buttons clicked, information typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from their health care providers.

152. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.[26] This information is disclosed to Facebook regardless of whether a user is logged into their Facebook account at the time.

153. The transmission is instantaneous—indeed Facebook often receives the information before the health care provider does.

154. The transmission is invisible.

155. The transmission is made without any affirmative action taken by the patient.

156. The transmission occurs without any notice to the patient that it is occurring.

157. Facebook collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users, allowing Facebook to target ads to a person who, for example, has used a patient portal and has exchanged communications about a specific condition, such as cancer.

158. The information Meta Pixel captures and discloses to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history, including the identifiable information of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.[27] When users enter a URL address into their web browser using the 'http' web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request

[26] *See, e.g., In re Facebook, Inc. Internet Tracking Litigation,* 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).

[27] *In re Facebook*, 956 F.3d at 596.

and where to find them. Thus, the URL provides significant information regarding a user's browsing history, including identifiable information for the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

159. These search terms and the resulting URLs divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's own platform. In this manner, Facebook tracks users' browsing histories on third-party websites and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.[28]

160. For example, if the Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifiable information like IP addresses, Facebook IDs, user agent information, device identifiers, and other data. All this personally identifiable data is available each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

161. These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.[29]

[28] *In re Facebook*, 956 F.3d at 596.

[29] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

162. In exchange for installing its Meta Pixel, Facebook provides website owners like Defendant with analytics about the ads they have placed on Facebook and Instagram and tools to target people who have visited its websites.[30]

163. The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.[31]

164. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

165. Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."[32] According to Facebook, the Meta Pixel is an analytics tool that allows businesses to measure the effectiveness of their advertising by understanding the actions people take on its websites."[33]

166. Facebook warns web developers that its Pixel enables Facebook "to match your website visitors to their respective Facebook User accounts."[34]

167. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website's persistent header) to reduce the chances of browsers or code blocking Pixel's execution and to ensure that visitors will be tracked.[35]

168. Once the Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as

[30] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[31] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

[32] https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/

[33] https://www.oviond.com/understanding-the-facebook-pixel

[34] https://developers.facebook.com/docs/meta-pixel/get-started

[35] https://developers.facebook.com/docs/meta-pixel/get-started

"optional values" set by the business website.[36] Facebook builds user profiles on users that include the user's real name, address, location, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, such as IP addresses and the Facebook ID. Meta Pixel tracks this data regardless of whether a user is logged into Facebook.

169. Facebook tracks non-Facebook users through its widespread internet marketing products and source code, and Mark Zuckerberg has conceded that the company maintains "shadow profiles" on nonusers of Facebook.[37]

170. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information. The information is sent in data packets, which include personally identifiable data.

171. For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data."[38] HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."[39] Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."[40]

172. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.[41]

[36] https://developers.facebook.com/docs/meta-pixel/

[37] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/

[38] https://developers.facebook.com/docs/meta-pixel/

[39] https://developers.facebook.com/docs/meta-pixel/

[40] https://developers.facebook.com/docs/meta-pixel/

[41] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

173. Facebook has a number of ways to exploit the data that is being forwarded from third-party websites through the Meta Pixel.

174. If a user has a Facebook account, the user data may be collected and linked to the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

175. Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."[42] The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.[43]

176. Facebook can also link user data to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching.[44] Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users' Facebook accounts.

177. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data.[45] In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.[46]

[42] https://clearcode.cc/blog/facebook-first-party-cookie-adtech/

[43] https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

[44] https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[45] https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[46] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

178. Facebook also receives personally identifiable information in the form of user's unique IP addresses, which remain the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

179. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is a means of identification that is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

180. An unskilled computer user can obtain the c_user value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse anywhere on the background of the page, (3) selecting 'View page source,' (4) executing a control-F function for "user=" and (5) copying the number value that immediately follows "user=" in the page source code of the target Facebook user's page.

181. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

182. The datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

183. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.

184. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Tracking Pixel program.

185. The fbp cookie emanates from Defendant's Web Properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy.

186. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as the "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.[47] These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.[48]

187. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like Defendant's website, and target users with advertising based on their web activity.

[47] https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.

[48] https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

188. Facebook then sells advertising space by highlighting its ability to target users. Facebook can target users so effectively because it surveils user activity both on and off its official website. This allows Facebook to make inferences about users far beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[49] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to create highly specific targeted advertising. Indeed, Facebook uses precisely the type of Personal Health Information that Defendant bartered to Facebook so that Facebook can identify, target, and market products and services to individuals.

F. Defendant has embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' and users' protected health information to Facebook.

189. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

190. Facebook's intrusion into the personal data of visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.[50] Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

191. Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through

[49] https://www.facebook.com/business/ads/ad-targeting

[50] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

future Facebook ads.[51] For example, websites can use this data to create "custom audiences" to target the specific Facebook user, as well as other Facebook users who match "custom audience's" criteria.[52] Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

192. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.[53] Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for advertising purposes.[54]

193. Recently, investigative journalists have determined that Meta Pixel is embedded on the websites of many of the top hospitals in the United States.[55] This results in sensitive medical information being collected and then sent to Facebook when a user interacts with these hospital websites.

194. For example, when a user on many of these hospital websites clicks on a "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term (such as "cardiology") used to find the doctor to Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

195. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, or logout of a patient portal or to create an appointment—Facebook code embedded on that page redirects the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

[51] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[52] https://developers.facebook.com/docs/marketing-api/reference/custom-audience/

[53] https://instapage.com/blog/meta-pixel

[54] https://instapage.com/blog/meta-pixel

[55] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

196. Defendant is among the hospital systems who have embedded Meta Pixel on their websites. Via its use of the Meta Pixel, Defendant intercepted and disclosed the contents of Plaintiff and Class Members' communications with Defendant, including the precise text of patient search queries and communications about specific doctors, communications about medical conditions and treatments, buttons clicked to Search, Find a Doctor, connect, Login, or Enroll in Defendant's patient portal, summaries of Defendant's responsive communications, the parties to the communications, appointment information, and the existence of communications at Defendant's websites.

197. For example, when a patient visits the homepage of Defendant's website, the source code employed by Defendant causes personally identifiable information to be transmitted to Facebook and Google.

198. Many of the tabs provided by Defendant on its website are specific to patients—i.e., "Find a Provider," "Patients and Visitors," "Health Care Services," "Education & Training," and "MyHealth Online," among others (collectively, "Patient Tabs"). Clicking on any of the Patient Tabs identifies the person using the website as a patient.

199. For example, when a patient enters their personal information through Defendant's websites that incorporate Meta Pixel, such as to locate a doctor, this information, including what the patient is being treated for, is immediately and instantaneously routed to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

200. This data, which can include health conditions (e.g., addiction, HIV, heart disease), diagnoses, procedures, test results, the treating physician, medications, as well as personally identifiable information (collectively, "Personal Health Information"), is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising.

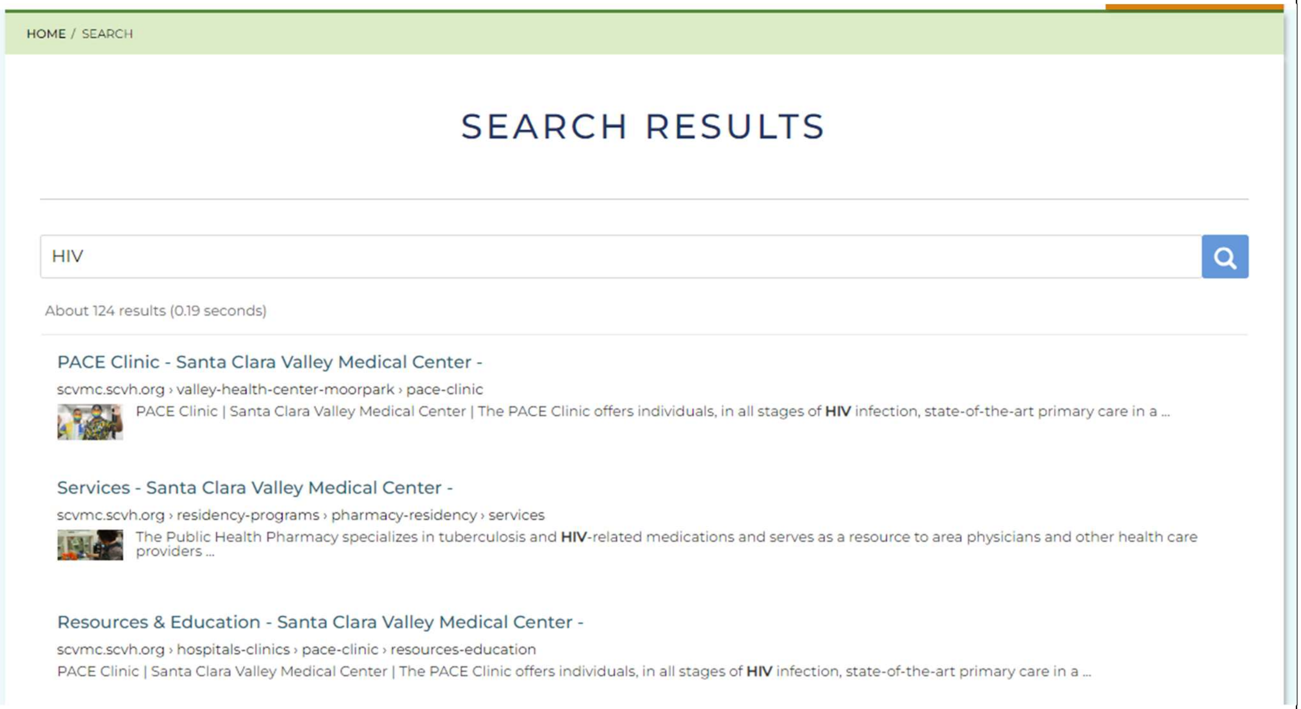
201. In addition, through the source code deployed by Defendant, Defendant provides third parties (including Facebook and Google) with other data, such as cookies that Defendant

uses to help Facebook identify patients. Those cookies include (but are not necessarily limited to) cookies named: c_user, datr, fr, and fbp.

202. For example, the fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Defendant's Web Properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. This data was disclosed to Facebook simultaneously in real time as visitors transmitted their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also disclosed other personally identifiable information to Facebook, such as patient and user IP addresses, cookie identifiers, browser-fingerprints, and device identifiers. Defendant also discloses the same kind of information to Google Analytics and Google Double Click every time a patient fills out the above form.

203. Defendant causes similar data transmissions to be sent to Facebook and Google with every communication that a patient sends using the Patient Tabs.

204. Defendant discloses such personally identifiable information and sensitive medical information even when patients or users are searching for doctors to assist them with treatments such as HIV:



SEARCH RESULTS

HIV

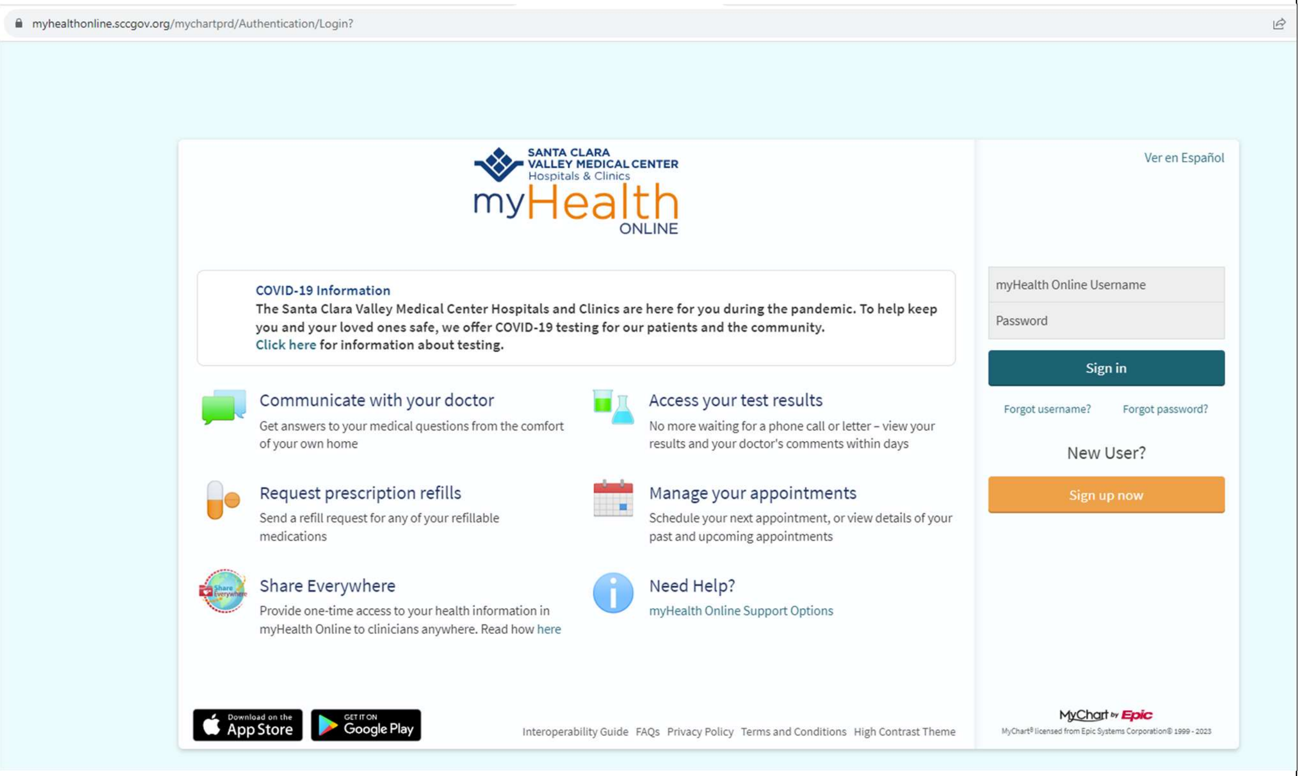
About 124 results (0.19 seconds)

PACE Clinic - Santa Clara Valley Medical Center -
scvmc.scvh.org › valley-health-center-moorpark › pace-clinic
PACE Clinic | Santa Clara Valley Medical Center | The PACE Clinic offers individuals, in all stages of **HIV** infection, state-of-the-art primary care in a ...

Services - Santa Clara Valley Medical Center -
scvmc.scvh.org › residency-programs › pharmacy-residency › services
The Public Health Pharmacy specializes in tuberculosis and **HIV**-related medications and serves as a resource to area physicians and other health care providers ...

Resources & Education - Santa Clara Valley Medical Center -
scvmc.scvh.org › hospitals-clinics › pace-clinic › resources-education
PACE Clinic | Santa Clara Valley Medical Center | The PACE Clinic offers individuals, in all stages of **HIV** infection, state-of-the-art primary care in a ...

205. Likewise, if a patient wants to access their medical records, schedule appointments, email their doctor, view lab results, or refill medications, they are required to do so through Defendant’s website patient portal—all while Defendant’s website tracks their activity:



myhealthonline.sccgov.org/mychartprd/Authentication/Login?

SANTA CLARA VALLEY MEDICAL CENTER Hospitals & Clinics

myHealth ONLINE

Ver en Español

COVID-19 Information

The Santa Clara Valley Medical Center Hospitals and Clinics are here for you during the pandemic. To help keep you and your loved ones safe, we offer COVID-19 testing for our patients and the community.

Click here for information about testing.

Communicate with your doctor

Get answers to your medical questions from the comfort of your own home

Access your test results

No more waiting for a phone call or letter – view your results and your doctor's comments within days

Request prescription refills

Send a refill request for any of your refillable medications

Manage your appointments

Schedule your next appointment, or view details of your past and upcoming appointments

Share Everywhere

Provide one-time access to your health information in myHealth Online to clinicians anywhere. Read how here

Need Help?

myHealth Online Support Options

myHealth Online Username

Password

Sign in

Forgot username? Forgot password?

New User?

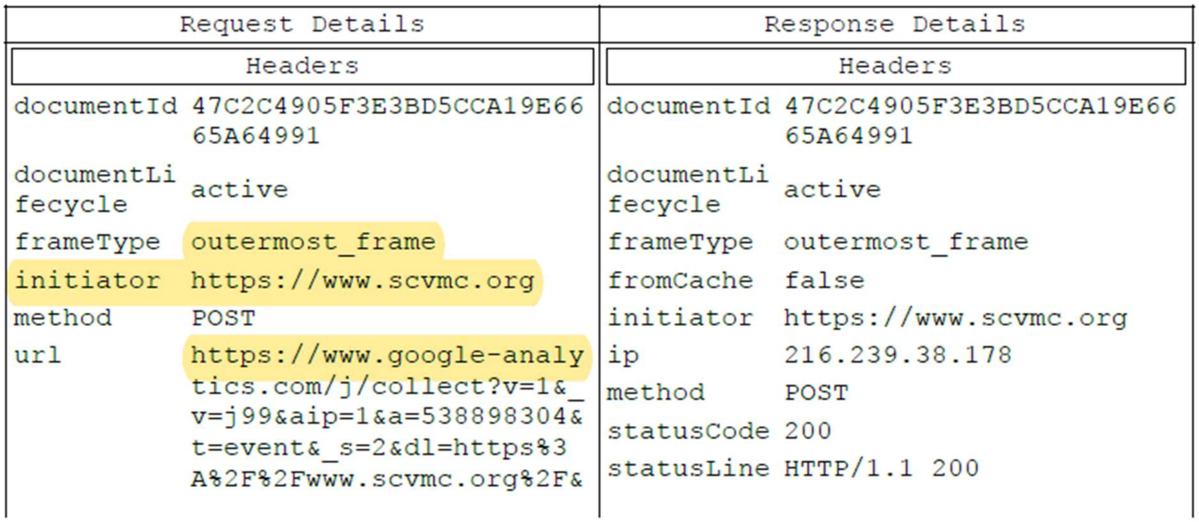
Sign up now

Interoperability Guide FAQs Privacy Policy Terms and Conditions High Contrast Theme

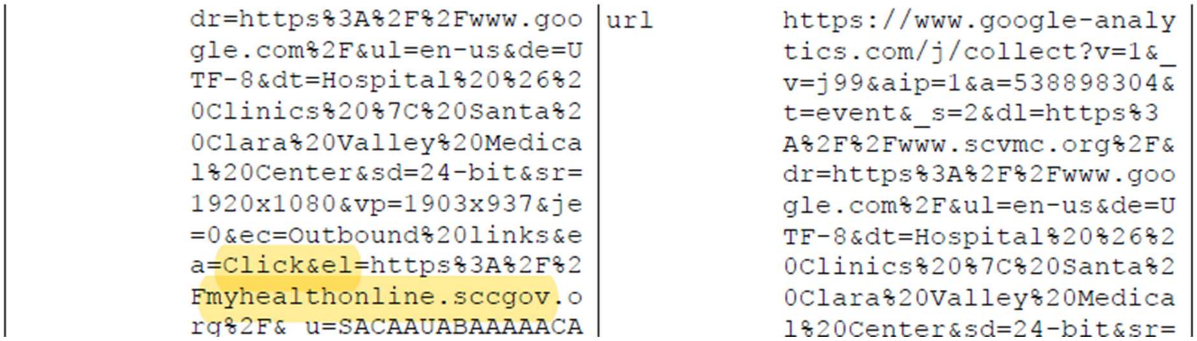
MyChart by Epic

MyChart® licensed from Epic Systems Corporation® 1999 - 2023

206. Each time a patient, including Plaintiff and Class Members, visited Defendant's patient portal, tracking pixels installed on the patient portal page and login button caused the patient's personal identifiers, including the patient's IP address, to be transmitted to Google and other third parties attached to the fact that the patient has exchanged a communication with Defendant regarding the patient portal:



Request Details		Response Details	
Headers		Headers	
documentId	47C2C4905F3E3BD5CCA19E6665A64991	documentId	47C2C4905F3E3BD5CCA19E6665A64991
documentLifecycle	active	documentLifecycle	active
frameType	outermost_frame	frameType	outermost_frame
initiator	https://www.scvmc.org	fromCache	false
method	POST	initiator	https://www.scvmc.org
url	https://www.google-analytics.com/j/collect?v=1&_v=j99&aip=1&a=538898304&t=event&_s=2&dl=https%3A%2F%2Fwww.scvmc.org%2F&	ip	216.239.38.178
		method	POST
		statusCode	200
		statusLine	HTTP/1.1 200



	dr=https%3A%2F%2Fwww.google.com%2F&ul=en-us&de=UTF-8&dt=Hospital%20%26%20Clinics%20%7C%20Santa%20Clara%20Valley%20Medical%20Center&sd=24-bit&sr=1920x1080&vp=1903x937&je=0&ec=Outbound%20links&ea=Click&el=https%3A%2F%2Fmyhealthonline.sccgov.org%2F&_u=SACAAUABAAAAACA	url	https://www.google-analytics.com/j/collect?v=1&_v=j99&aip=1&a=538898304&t=event&_s=2&dl=https%3A%2F%2Fwww.scvmc.org%2F&dr=https%3A%2F%2Fwww.google.com%2F&ul=en-us&de=UTF-8&dt=Hospital%20%26%20Clinics%20%7C%20Santa%20Clara%20Valley%20Medical%20Center&sd=24-bit&sr=

207. On information and belief, the Defendant patient portal is designed to permit the deployment of custom analytics scripts within the patient portal, including Google Analytics, which allows for the transmission of patients' Personal Health Information, including medical and health-related information, and communications to third parties.

208. On information and belief, Defendant took advantage of the patient portal's analytics compatibility by knowingly and secretly deploying Google source code inside its patient portal that caused the contemporaneous unauthorized transmission of Personal Health Information and the precise content of patient communications with Defendant to be sent to Google whenever

a patient used the patient portal, including when Plaintiff used Defendant's patient portal in June 2023 to communicate with her doctor and view test results.

209. All this information is acquired by Defendant and forwarded to third parties, including Google, via tracking devices that Defendant has installed on its Web Properties.

210. When a patient sends a communication searching for more information about their condition, Defendant causes data transmissions to be made to third parties, including Facebook and Google, which include Personal Health Information, including personally identifiable information and the content of the patient's communications.

211. In other words, Facebook learns not just that patients are seeking treatment, but where and typically when they are seeking treatment, along with other information that patients would reasonably assume that Defendant is not sharing with third party marketing companies.

212. Defendant also discloses patient information from across its website at https://scvmc.scvh.org including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for services offered by Defendant, communications made by patients making appointments, communications made when patients access Defendant's patient portal, and communications made when patients are researching specific medical conditions such as COVID-19.

213. Despite its own legal obligations and internal policies, Defendant's source code causes the interception and transmission of the following personally identifiable information ("PII") to third parties whenever a patient uses Defendant's Web Properties, including on its website and patient portal:

a. Patient IP addresses;

b. Unique, persistent patient cookie identifiers;

c. Device identifiers;

d. Account numbers;

e. URLs;

f. Other unique identifying numbers, characteristics, or codes, including patients' Facebook IDs; and

g. Browser-fingerprints.

214. To make the transmissions of patient information and communications to Facebook and Google, Defendant deployed Facebook and Google source code on its Web Properties.

215. The Defendant-deployed source code did the following things:

a. Without any action or authorization, Defendant deposited cookies such as the _fbp, _ga, and _gid cookies onto Plaintiff's and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiff's and Class Members' computing devices by disguising them as first-party cookies.

b. Without any action or authorization, Defendant's source code commanded Plaintiff's and Class Members' computing devices to contemporaneously re-direct the Plaintiff's and Class Members' identifiers and the content of their communications to Facebook, Google, and others.

216. Whenever a patient uses Defendant's Web Properties, Defendant intercepts, causes transmission of, and uses personally identifiable patient data without patient knowledge, consent, authorization, or any further action by the patient.

217. Defendant disclosed Plaintiff's and Class Members' personally identifiable patient data, including their status as patients and the contents of their communications with Defendant, to third parties including Facebook and Google.

218. Defendant's unauthorized disclosures to third parties includes information that identifies Plaintiff and Class Members as patients of Defendant and aids the third parties in

receiving and recording patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to Defendant's patient portal.

219. Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed), and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

220. The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Defendant's websites. The path identifies where a file can be found on a website. For example, a patient reviewing information about the "Services" that Defendant offers patients such as information about Covid-19 will generate a URL with the path https://scvmc.scvh.org/patients-visitors/services/covid-19-oral-antiviral.

221. Likewise, a query string provides a list of parameters. An example of a URL that provides a query string is https://scvmc.scvh.org/search?q=HIV. The query string parameters in this search indicate that a search was done at Defendant's website for information about chemotherapy. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider.

222. Defendant also provides Facebook and Google with details about online forms that patients fill out in the form of POST requests. All the information that patients provide when filling out these forms is also disclosed to Facebook and Google.

223. As the above demonstrates, knowing what information a patient is reviewing on Defendant's website can reveal deeply personal and private information. For example, a simple search for "pregnancy" on Defendant's website tells Facebook that the patient is likely pregnant. Indeed, Facebook might know that the patient is pregnant before the patient's close family and

friends. But there is nothing visible on Defendant's website that would indicate to patients that, when they use Defendant's search function, their personally identifiable information and the precise content of their communications with Defendant are being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

224. The amount of data collected is significant. Via the Meta Pixel, when patients interact with its website, Defendant discloses a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient types a search term into the search bar on Defendant's website, the website returns links to information relevant to the search term. When patients then click these links, a communication is created that contains a GET request and a full-string detailed URL.

225. The contents of patients' search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Defendant's website. Worse, no matter how sensitive the area of the Defendant's website that a patient reviews, the referral URL is acquired by Facebook along with other personally identifiable information.

226. The nature of the collected data is also important. Defendant's unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient's medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Defendant's website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

227. Defendant also discloses the same kind of patient data described above to other third parties involved in internet marketing, including Google, YouTube, and New Relic, via

tracking software that Defendant has installed on its website. As with the Facebook Meta Pixel, Defendant provides patients and prospective patients with no notice that Defendant is disclosing the contents of their communications to these third parties. Likewise, Defendant does not obtain consent from patients and prospective patients before forwarding their communications to these companies.

228. These disclosures to third parties other than Facebook are equally disturbing. Google Analytics, for example, has been described by the Wall Street Journal as "far and away the web's most dominant analytics platform," which "tracks you whether or not you are logged in."[56] Like Facebook, Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers. Defendant routinely discloses patients' Personal Health Information to such Google services as Google Analytics, Google DoubleClick, and Google AdWords.

229. Google cookies are personally identifiable. For example, Google cookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time.

230. Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information.

231. Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, Google uses such cookies to remember your users' most recent searches, previous interactions with an advertiser's ads or search results, and visits to an advertiser's website. This helps Google show customized ads to users on Google.

232. Google also uses one or more cookies for advertising it serves across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers

[56] https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401

under the domain doubleclick.net. Another is stored in google.com and is called ANID. Google also uses other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show users ads.

233. Google cookies provide personally identifiable data about patients who visit Defendant's website to Google. Defendant transmits personally identifiable Google cookie data to Google.

234. Google warns web-developers that Google marketing tools are not appropriate for health-related webpages and websites. Indeed, Google warns web developers that "Health" is a prohibited category that should not be used by advertisers to target ads to users or promote advertisers' products or services.

235. Google cookies are personally identifiable. For example, Google cookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time.

236. Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information.

237. Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, Google uses such cookies to remember your users' most recent searches, previous interactions with an advertiser's ads or search results, and visits to an advertiser's website. This helps Google show customized ads to users on Google.

238. Google also uses one or more cookies for advertising it serves across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. Google also uses other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show users ads.

239. Defendant deploys Google tracking tools on nearly every page of its websites, resulting in the disclosure of communications exchanged with patients to be transmitted to Google. These transmissions occur simultaneously with patients' communications with Defendant and include communications that Plaintiff and Class Members made about specific medical providers, treatments, conditions, appointments, payments, and registrations and logins to Defendant's patient portal.

240. By compelling visitors to its websites to disclose personally identifiable data and sensitive medical information to Facebook, Defendant knowingly discloses information that allows Facebook and other advertisers to link patients' and visitors' Personal Health Information to their private identities and target them with advertising (or do whatever else Facebook may choose to do with this data, including running "experiments" on its customers by manipulating the information they are shown on their Facebook pages).[57] Defendant intentionally shared the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

241. Defendant facilitated the disclosure of Plaintiff's Personal Health Information, including sensitive medical information, to Facebook without her consent or authorization when he entered information on the website that Defendant maintains at https://scvmc.scvh.org/home.

242. For example, Plaintiff Jane Doe is an individual with a Facebook account who is also a patient of Defendant and who has received treatment by Defendant's doctors at Defendant's medical facilities. Plaintiff has been a Santa Clara Valley Medical Center patient since 2017. Plaintiff has visited Defendant's website since 2018, including in June 2023, and entered data, including sensitive medical information, such as details about her medical condition. Plaintiff has regularly used Defendant's patient portal since 2017. The information that Plaintiff transmitted included queries about treatment for cirrhosis of liver and ascites, generalized anxiety disorder,

[57] https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

migraines, and carpal tunnel syndrome. The treatments that Plaintiff explored on Defendant's website included psychiatric treatment, physical therapy, and pain management. She also used Defendant's website to search for a neurologist.

243. Throughout, Plaintiff has also used Defendant's patient portal to schedule appointments, order medications, view test results, and message her doctor.

244. In addition to using the Defendant's patient portal (whose login button was embedded with a tracking pixel), when interacting with the Defendant's website and patient portal, Plaintiff also communicated such specific details as her name, her patient status, the name of her specific treating physician, her browsing history, and the name of the specific medical conditions that she was seeking treatment for.

245. This information could then be combined with other information in Facebook's possession, like her name, date of birth, and phone number, to more effectively target Plaintiff with advertisements or sell Plaintiff's data to third parties.

246. Because Defendant embedded the Meta Pixel on its website, Defendant disclosed intimate details about Plaintiff's interactions with its website, including Plaintiff's scrolling, typing, and selecting options from drop down menus. Each time the Meta Pixel was triggered, it caused Plaintiff's information to be secretly transmitted to Facebook's servers, as well as additional information that captures and discloses the communications' content and Plaintiff's identity. For example, when Plaintiff and Class Members visited Defendant's website, their Personal Health Information was transmitted to Facebook, including such engagement as using the website's search bar, using the website's Find a Doctor function, and typing content into online forms. During these same transmissions, Defendant's website would also provide Facebook with Plaintiff's and Class Members' Facebook ID, IP addresses, device IDs, and other information that Plaintiff and Class Members provided. This is precisely the type of information that state and federal law require healthcare providers to de-identify to protect the privacy of patients.

247. Facebook and Google used the data provided by Defendant to send Plaintiff targeted advertising related to her medical conditions. Indeed, after visiting Defendant's website, Plaintiff began receiving targeted advertising on her Facebook page related to her medical conditions, including advertisements for pain management, other advertisements for medications for her various conditions, and solicitations to participate in research questionnaires, research studies, and clinical trials.

248. Because Defendant embedded the Meta Pixel on its websites, Defendant disclosed intimate details about Plaintiff's and the Class Members interactions with its websites, including when Plaintiff and Class Members selected options from drop down menus.

249. One or more persons at Facebook and Google viewed Plaintiff's and Class Members' Personal Health Information as a consequence of Defendant's installation of the Meta Pixel on its Web Properties. After Plaintiff's and Class Members' Personal Health Information had been intercepted and collected, individuals at Facebook processed, analyzed, and assimilated Plaintiff's and Class Members' Personal Health Information into data sets like "Core Audiences" and "Custom Audiences" for the purpose of targeting Plaintiff and Class Members with advertising.

250. Defendant knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' Personal Health Information, including sensitive medical information and personally identifying data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant was also aware that installing the Meta Pixel tool would result in one or more unauthorized persons at Facebook and Google viewing the Personal Health Information of Defendant's patients, including the Personal Health Information of Plaintiff and Class Members. Defendant's decision to affirmatively communicate and share their patients' Personal Health Information with Facebook, Google, and those companies' employees violates the numerous protections afforded by California law.

251. Defendant also knew that installing the Meta Pixel on its website would result in its patients' Personal Health Information being improperly accessed by Facebook and its employees so that Facebook could sell advertising. Defendant made the decision to barter its patients' Personal Health Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it also violated the privacy rights of Plaintiff and Class Members.

G. Defendant's interception and disclosure of patient communications permits Facebook, Google, and other third-party advertising companies to engage in cross-device targeting across multiple devices.

252. In addition to enabling Defendant to advertise to patients and potential patients on non-Defendant websites, Defendant's misuse and exploitation of patient data and communications also facilitates third parties' ability to target advertisements on other computing devices that a patient uses. This is called cross-device targeting.

253. Third parties including Facebook and Google have established a unique ID for individuals that tie together their desktop, laptop, and smartphone computing devices. For example, even if a patient has never visited Defendant's website on their smartphone, cross-device tracking and marketing allows Defendant and other third parties to target patients on that device. In other words, a patient or potential patient who visited Defendant's website on his desktop, but never on his smartphone, can nevertheless be targeted with advertisements by both Defendant and other third parties on his smartphone.

254. Defendant's and other third parties' use of cross-device targeting demonstrates that the data Defendant discloses to third parties is personally identifiable because it enables patients to be tracked across multiple devices that patients own—even if a patient has never communicated with Defendant on one or more of their devices.

255. Defendant has made the decision that access to the targeted advertising (including retargeting and cross-device tracking) that is enabled by its disclosure of patient data and communications is of commercial benefit to Defendant.

256. Defendant obtains additional revenue from its deployment of third-party tracking tools through which it discloses personally identifying patient data and communications to third parties, including Google and Facebook.

257. Any additional revenue that that Defendant obtained from its unauthorized misuse of its own patients' Personal Health Information is unearned and is the rightful property of the patients (including Plaintiff and Class Members) from whom it was obtained.

258. Defendant's unauthorized disclosure and misuse of Plaintiff's and Class Members' Personal Health Information is a form of theft, for which the victims are entitled to recover anything acquired with the stolen assets, even if the items acquired have a value that exceeds the value of that which was stolen.

H. Plaintiff and the Class Members did not consent to the interception and disclosure of their Protected Health Information.

259. Plaintiff and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, the Meta Pixel tool is seamlessly and secretly integrated into Defendant's websites and is invisible to patients visiting those websites.

260. For example, when Plaintiff visited Defendant's website in 2023, there was no indication her Personal Health Information was being collected, transmitted, and monitored by Facebook for advertising purposes.

261. Plaintiff and her fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook, Google, and other third parties for the purpose of targeting them with advertising.

262. Moreover, it is against the law for Defendant to disclose individually identifying health information without giving appropriate notice to the patient and obtaining written consent.

263. Defendant does not have a legal right to share Plaintiff's and Class Members' Protected Health Information ("PHI") with Facebook, because this information is protected from such disclosure by law. *See, e.g.*, CAL. CIV. CODE §§ 56 *et seq.*; 45 C.F.R. § 164.508. Nor is Defendant permitted to disclose patients' Protected Health Information to an advertising and marketing company like Facebook without express written authorization from patients.

264. Indeed, the United States Department of Health and Human Services ("HHS") recently confirmed that hospitals are prohibited from transmitting individually identifiable health information via tracking technology like the Meta Pixel without a patient's authorization and other protections like a business associate agreement with the recipient of the patient data:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[58]

265. The disclosure of Plaintiff's and class members' Personal Health Information via the tracking pixels contravenes both the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Personal Health Information.

266. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, **discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.** Such disclosures can reveal incredibly sensitive information about an individual, **including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.** While

[58] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited June 12, 2023).

> it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**[59]

267. Plaintiff and Class Members face the same risks the government is warning about. Defendant has shared Plaintiff's and Class Members' search terms about health conditions for which they seek doctors; their contacts with doctors to make appointments; the names of their doctors; the frequency with which they take steps to obtain healthcare for certain conditions; and where they seek medical treatment. This information is, as described by the OCR bulletin, "highly sensitive." The Bulletin goes on to make clear how broad the government's view of protected information is.

268. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[60]

269. Crucially, that paragraph in the government's Bulletin continues:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[61]

[59] *Id.* (emphasis added).

[60] *Id.* (emphasis added).

[61] *Id.*

270. On July 20, 2023, the Federal Trade Commission, acting in concert with the United States Department of Health and Human Services' Office for Civil Rights, sent letters to approximately 130 hospital systems and telehealth providers to alert them "to the serious privacy and security risks related to the use of online tracking technologies" on hospital websites which have been "impermissibly disclosing consumers' sensitive health information to third parties."[62]

271. The FTC's letter specifically warned hospitals that "use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities" can result in "a wide range of harms to an individual or others", including the disclosure of "health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[63] The FTC's letter further warned hospitals that "HIPAA rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (*e.g.* tracking technology vendors) includes PHI. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA rules."[64]

272. That same day the FTC issued a bulletin warning that even companies not covered by HIPAA have a responsibility to protect against the unauthorized disclosure of Personal Health Information and cautioning that the "unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule."[65]

273. Defendant failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications by third parties for their own direct marketing uses.

[62] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[63] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[64] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[65] https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking

Moreover, no *additional* privacy breach by Facebook is necessary for harm to have accrued to Plaintiff and Class Members; the secret disclosure by Defendant of its patients' Personal Health Information to Facebook means that a significant privacy injury has *already occurred.*

274. Likewise, a prospective or current patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Such "Browser-Wrap" statements do not create an enforceable contract against consumers.

275. Neither Plaintiff nor Class Members knowingly consented to Defendant's disclosure of their Personal Health Information to Facebook. Nowhere in Defendant's privacy policy is it disclosed that Defendant routinely transmits patients' Personal Health Information to third party advertising companies like Facebook so that those companies can monetize and exploit patients' health data for advertising purposes. Without disclosing such practices, Defendant cannot have secured consent from Plaintiff and Class Members for the disclosure of their Personal Health Information to Facebook and other third-party advertising companies.

276. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiff's and Class Members' Personal Health Information to Facebook or aid in the same.

I. The disclosure of personal patient data to Facebook is unnecessary.

277. There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are the disclosures of patient Personal Health Information to Facebook necessary for Defendant to maintain their healthcare website or provide medical services to patients.

278. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Health Information to companies like Facebook.

Likewise, it is possible for Defendant to provide medical services to patients without sharing their Personal Health Information with Facebook so that this information can be exploited for advertising purposes.

279. Despite these possibilities, Defendant willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third parties, including Facebook and Google.

J. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, especially with respect to sensitive medical information.

280. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, including personally identifiable data and sensitive medical information. Defendant's surreptitious interception, collection, and disclosure of Personal Health Information to Facebook violated Plaintiff and Class Members' privacy interests.

281. As a patient, Plaintiff and Class Members had a reasonable expectation of privacy that her health care provider and its associates would not disclose their Personal Health Information to third parties without their express authorization. Those expectations are derived from multiple sources, including (a) Defendant's status as Plaintiff's and Class Members' health care provider, (b) Defendant's common law obligations to maintain the confidentiality of patient data and communications, (c) state and federal laws and regulations protecting the confidentiality of medical information, (d) state and federal laws protecting the confidentiality of electronic communications and computer data, and (e) state laws protecting unauthorized use of personal means of identification.

282. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[66]

[66] *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671 n.1 (Mo. 1993).

283. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[67] Likewise, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications. For example, the AMA has issued medical ethics opinions providing that

> Protecting information gathered in association with the care of a patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust….Physicians must seek to protect patient privacy in all settings to the greatest extent possible and should … [m]inimize intrusion on privacy when the patient's privacy must be balanced against other factors [and inform] the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware."[68]

284. The AMA's ethics opinions have further cautioned physicians and hospitals that "[d]isclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship." [69]

285. Patient health information is specifically protected by law. The prohibitions against disclosing patient Personal Health Information include prohibitions against disclosing personally identifiable data such as patient names, IP addresses, and other unique characteristics or codes. *See, e.g.*, CAL. CIV. CODE § 56.05 ("medical information"); 45 C.F.R. § 164.514.

286. Plaintiff and Class Members' reasonable expectations of privacy in their Personal Health Information are grounded in, among other things, Defendant's status as a health care provider, Defendant's common law obligation to maintain the confidentiality of patients' Personal Health Information, state and federal laws protecting the confidentiality of medical information,

[67] https://www.pbs.org/wgbh/nova/doctors/oath_modern.html

[68] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.1.1).

[69] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.2.4).

state and federal laws protecting the confidentiality of communications and computer data, and state laws prohibiting the unauthorized use and disclosure of personal means of identification.

287. Given the application of these laws to Defendant, Plaintiff and the Members of the Class had a reasonable expectation of privacy in their Protected Health Information.

288. Indeed, several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

289. Polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

290. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[70]

291. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[71]

292. "Patients are highly sensitive to disclosure of their health information," particularly because it "often involves intimate and personal facts, with a heavy emotional overlay."[72] Unsurprisingly, empirical evidence demonstrates that "[w]hen asked, the

[70] https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/

[71] https://www.wired.co.uk/article/apple-ios14-facebook

[72] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002).

overwhelming majority of Americans express concern about the privacy of their medical records."[73]

293. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[74]

294. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's Personal Health Information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

K. Plaintiff's and Class Members' Personal Health Information that Defendant collected, disclosed, and used has economic value, and its disclosure has caused Plaintiff and Class Members harm.

295. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiff and Class Members have a vested property right in their Personal Health Information.

296. The United States Supreme Court has explained that, "Confidential business information has long been recognized as property." *Carpenter v. United States*, 484 U.S. 19, 26 (1987). "Depriv[ation] of [the] right to exclusive use of … information" causes a loss of property "for exclusivity is an important aspect of confidential business information and most private

[73] Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKLEY TECH L.J. 1523, 1557 (2009).

[74] https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/

property for that matter." *Id*. at 27. There is no doubt that Defendant has a "property right" in patient data such that, if Facebook or Google took such information from Defendant without authorization, Defendant would have a claim for Facebook and Google's taking of their property. Patients also have a property right in their own health information that may not be taken or used by Defendant Rush without their authorization for non-health care related reasons.

297. Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

298. A patient's right to protect the confidentiality of their health data and restrict access to it is a valuable right.

299. In addition to property rights in their health data, patients enjoy property rights in the privacy of their health communications.

300. Patient property rights in their health data and communications are established by HIPAA and state health privacy laws that are equally or more stringent than HIPAA, including CIMA.

301. Defendant's unauthorized acquisition, use, and disclosure of Plaintiff's and Class Members' individual Personal Health Information for marketing purposes violated their property rights to control how their health data and communications are used and who may be the beneficiaries of their data and communications.

302. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Defendant has collected and disclosed from Plaintiff and Class Members. Indeed, the value of data that companies like Facebook and Google extract from people who use the Internet is well understood and generally accepted in the e-commerce industry.

303. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information. Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV. L. REV. 2055, 2056-57 (2004).

304. For example, in 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."

305. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price." This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 to $164 per year between 2013 and 2020.

306. Medical information derived from medical providers garners even more value from the fact that it is not available to third party data marketing companies because of strict restrictions on provider disclosures under HIPAA, state laws, and provider standards, including the Hippocratic oath.

307. The cash value of Internet users' Personal Health Information can be quantified. In a 2015 study by the Ponemon Institute, researchers determined the value that American Internet users place on their "health condition" as more valuable than any other piece of data about them, with a minimum value of $82.90.[75]

308. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name. That same article noted that "Data has become a strategic asset that allows

[75] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at https://vdocuments.site/privacy-and-security-in-a-connected-life-protect-personal-information-from-being.html?page=1.

companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.

309. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health care providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.

310. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.

311. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.

312. Defendant was compensated for its disclosures of Plaintiff's and Class Members' personally identifiable patient data and communications by the third-party recipients in the form of enhanced marketing services or other compensation.

313. Defendant did not pay or offer to pay Plaintiff or Class Members for their communications or personally identifiable patient data associated with these disclosures before or after the disclosures were made.

314. Defendant profited from Plaintiff's and Class Members' information without ever intending to compensate Plaintiff and Class Members or inform them that the disclosures had been made.

315. Defendant was unjustly enriched by its conduct.

316. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiff and the Class Members of the

economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff and the Class Members' property.

L. Defendant's failure to inform its patients and prospective patients that their Personal Health Information has been disclosed to Facebook or to take any steps to halt the continued disclosure of patients' Personal Health Information is malicious, oppressive, and in reckless disregard of Plaintiff and Class Members' rights.

317. Hospital systems, like other businesses, have a legal obligation to disclose data breaches to their customers. *E.g.* CAL. CIV. CODE § 1798.82.

318. Defendant's decision to hide its use of the Meta Pixel tool from its own patients and its refusal to remove all such technologies from its websites even after learning that its patients' Personal Health Information was being routinely collected, transmitted, and exploited by Facebook, Google, and other third parties is malicious, oppressive, and in reckless disregard of Plaintiff's and Class Members' rights.

M. Tolling, Concealment, and Estoppel

319. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

320. Defendant seamlessly and secretively incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

321. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct, because there were no disclosures or other indication that Defendant was sharing their Personal Health Information with companies like Facebook, so that Facebook could exploit their Personal Health Information via targeted advertising campaigns.

322. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of patients' and users' Personal Health Information has continued unabated through the date of the filing of this complaint. What's more, Defendant was under a duty to disclose the nature and significance of its data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

VII. CLASS DEFINIITION

323. Defendant's conduct violates the law.

324. Defendant's unlawful conduct has injured Plaintiff and Class Members.

325. Defendant's conduct is ongoing.

326. Plaintiff brings this action individually and as a class action against Defendant.

327. Plaintiff brings this action in accordance with Federal Rule of Civil Procedure 23 individually and on behalf of the following proposed Class and Subclass:

> **Santa Clara Valley Medical Center Class:** For the period August 25, 2018, to the present, all patients or prospective patients of Defendant or any of its affiliates who exchanged communications at Defendant's websites, including https://scvmc.scvh.org and any other Defendant-affiliated website, including Defendant's patient portals.
>
> **The Patient Subclass:** For the period August 25, 2018, to the present all patients of Defendant or any of its affiliates and who exchanged communications at Defendant's websites, including https://scvmc.scvh.org and any other Defendant affiliated website, including Defendant's patient portals.

328. Excluded from the Class and Subclass are: (1) any Judge or Magistrate presiding over this action or appellate judge assigned to this case and any members of their staff and immediate families; (2) any jurors assigned to hear this case as well as their immediate families; (3) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers, and directors; and (4) Plaintiff's counsel and Defendant's counsel.

329. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance requirements for suing as representative parties.

330. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals. The exact number of Class Members can be determined by review of information maintained by Defendant. The proposed class is defined objectively in terms of ascertainable criteria.

331. **Predominant Common Questions:** The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to, the following:

(a) Whether Defendant violated Plaintiff's and Class Members' privacy rights;

(b) Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, CIVIL CODE §§ 56, *et seq.*;

(c) Whether Plaintiff and the Class Members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement; and,

(d) Whether Plaintiff and the Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

332. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories.

333. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is in conflict with the interests of the Class, and Defendant has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and she has the resources to do so.

Neither Plaintiff nor her counsel has any interest adverse to the interests of the other members of the Class.

334. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

335. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

VIII. CLAIMS FOR RELIEF

COUNT I—VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA") CAL. PENAL CODE §§ 630, *ET SEQ.*

336. Plaintiff re-alleges and incorporates all preceding paragraphs.

337. Plaintiff brings this claim on behalf of herself and all members of the Santa Clara Valley Medical Center Class.

338. The California Legislature enacted the California Invasion of Privacy Act, CAL. PENAL CODE §§ 630, *et seq*. ("CIPA") finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

339. CAL. PENAL CODE § 631(a) generally prohibits individuals, businesses, and other legal entities from "aid[ing], agree[ing] with, employ[ing], or conspir[ing] with" a third party to

read, attempt to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or to use, or attempt to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained.

340. CAL. PENAL CODE § 632(a) generally prohibits individuals, businesses, and other legal entities from recording confidential communications without consent of all parties to the communication.

341. All alleged communications between Plaintiff or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

342. Defendant used a recording device to record the confidential communications without the consent of Plaintiff or Class Members and then transmitted such information to others, such as Facebook.

343. The private information that Defendant assisted Facebook, Google, and other third parties with reading, learning, and exploiting, including Plaintiff's and Class Members' medical conditions, their medical concerns, and their past, present, and future medical treatment.

344. At all relevant times, Defendant's aiding Facebook to learn the contents of communications and Defendant's recording of confidential communications was without authorization and consent.

345. The Plaintiff and Class Members had a reasonable expectation of privacy regarding the confidentiality of their communications with Defendant. Defendant never sought to, or did, obtain Plaintiff's and Class Members' consent to transmit their Personal Health Information to Facebook.

346. Defendant engaged in and continues to engage in interception by aiding others (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire communications.

347. The intercepting devices used in this case include, but are not limited to:

(a) Plaintiff and Class Members' personal computing devices;

(b) Plaintiff and Class Members' web browsers;

(c) Plaintiff and Class Members' browser-managed files;

(d) Facebook's Meta Pixel;

(e) Internet cookies;

(f) Defendant's computer servers;

(g) Third-party source code utilized by Defendant; and

(h) Computer servers of third parties (including Facebook) to which Plaintiff and Class Members' communications were disclosed.

348. Defendant aided in, and continues to aid in, the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

349. Defendant aided in the interception of "contents" in at least the following forms:

(a) The parties to the communications;

(b) The precise text of patient search queries;

(c) Personally identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

(d) The precise text of patient communications about specific doctors;

(e) The precise text of patient communications about specific medical conditions;

(f) The precise text of patient communications about specific treatments;

(g) The precise text of patient communications about scheduling appointments with medical providers;

(h) The precise text of patient communications about billing and payment;

(i) The precise text of specific buttons on Defendant's website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

(j) The precise dates and times when patients click to Log-In on Defendant's website(s);

(k) The precise dates and times when patients visit Defendant's websites;

(l) Information that is a general summary or informs third parties of the general subject of communications that Defendant send back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

(m) Any other content that Defendant has aided third parties in scraping from webpages or communication forms at its Web Properties.

350. Plaintiff and Class Members reasonably expected that their Personal Health Information was not being intercepted, recorded, and disclosed to Facebook.

351. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Personal Health Information to Facebook. Neither Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by Defendant to Facebook. Nor could they have consented, given that Defendant never sought Plaintiff's or Class Members' consent, or even told visitors to its websites that their every interaction was being recorded and transmitted to Facebook via the Meta Pixel tool.

352. Defendant gave substantial assistance to Facebook in violating the privacy rights of Defendant's patients, despite the fact that Defendant's conduct constituted a breach of the

duties of confidentiality that medical providers owe their patients. Defendant knew that the installation of the Meta Pixel on its website would result in the unauthorized disclosure of its patients' communications to Facebook, yet nevertheless did so anyway.

353. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Personal Health Information, including using their sensitive medical information to develop marketing and advertising strategies.

354. Plaintiff and the Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

355. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

356. Plaintiff and Class Members have also suffered irreparable injury from Defendant's unauthorized acts of disclosure. Their personal, private, and sensitive data has been collected, viewed, accessed, stored, and used by Defendant and Facebook without their consent and has not been destroyed. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights. Plaintiff continues to desire to search for health information on Defendant's website. Plaintiff will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Defendant's website to search for health information in the future. Due to the continuing threat of injury, Plaintiff and Class Members have no adequate remedy at law, and Plaintiff and Class Members are therefore entitled to injunctive relief.

357. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT II—VIOLATION OF CMIA CIVIL CODE § 56.101

358. Plaintiff re-alleges and incorporates all preceding paragraphs.

359. Plaintiff brings this claim on behalf of herself and all members of the Patient Subclass.

360. Civil Code § 56.101, subdivision (a) requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

361. Any health care provider who "negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

362. Defendant failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to Facebook Plaintiff's and Subclass Members' sensitive medical information without consent,

including information concerning their health status, medical diagnoses, treatment, and appointment information, as well as personally identifiable information.

363. Defendant's failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information was, at the least, negligent and violates Civil Code § 56.36 subdivisions (b) and (c).

364. Accordingly, Plaintiff and Subclass Members may recover: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

365. In addition to statutory damages, Defendant's breach caused Plaintiff and Subclass Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Subclass Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Subclass Members and derived benefit therefrom without Plaintiff's and Subclass Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Subclass Members' personal information.

366. Plaintiff and Subclass Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III—VIOLATION OF CMIA CIVIL CODE § 56.10

367. Plaintiff re-alleges and incorporates all preceding paragraphs.

368. Plaintiff brings this claim on behalf of herself and all members of the Patient Subclass.

369. Civil Code § 56.10, subdivision (a), prohibits a health care provider from disclosing medical information without first obtaining an authorization, unless a statutory exception applies.

370. Defendant disclosed medical information without first obtaining authorization when it disclosed Plaintiff's and Subclass Members' sensitive medical information to Facebook without consent, including information concerning their health status, medical diagnoses, treatment, and appointment information, as well as personally identifiable information. No statutory exception applies. As a result, Defendant violated Civil Code § 56.10, subdivision (a).

371. Defendant knowingly and willfully, or negligently, disclosed medical information without consent to Facebook for financial gain.

372. Accordingly, Plaintiff and Subclass Members may recover: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); (4) punitive damages pursuant to 56.35; and (5) reasonable attorney's fees and other litigation costs reasonably incurred.

373. In addition to statutory damages, Defendant's breach caused Plaintiff and Subclass Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Subclass Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Subclass Members and derived benefit therefrom without Plaintiff's and Subclass Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff's and Subclass Members' personal information.

374. Plaintiff and Subclass Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IV—VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA") CAL. PENAL CODE § 502

375. Plaintiff re-alleges and incorporates all preceding paragraphs.

376. Plaintiff brings this claim on behalf of herself and all members of the Santa Clara Valley Medical Center Class.

377. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502 ("CDAFA") to "expand the degree of protection . . . from tampering, interference, damage, and unauthorized access to [including the extraction of data from] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . ." CAL. PENAL CODE § 502(a).

378. Under CDAFA, any person who "[k]nowingly accesses and without permission … *uses* any data … or computer system in order to either (A) devise or execute any scheme or artifice

to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data" is "guilty of a public offense." CAL. PENAL CODE § 502(c)(1).

379. Plaintiff's and the Class Members' devices on which they accessed the hospital or patient portals, including their computers, smart phones, and tablets, constitute computers or "computer systems" within the meaning of CDAFA. CAL. PENAL CODE § 502(b)(5).

380. Defendant violated section 502, subsection (c)(1)(A) by knowingly using data obtained from their patients as part of a scheme to defraud and deceive patients into surrendering their Personal Health Information so that Defendant could then barter that information to Facebook in return for economic benefits. Defendant violated section 502, subsection (c)(1)(B) by knowingly using data obtained from their patients to wrongfully obtain financial and other benefits from Facebook and Google by bartering patients' Personal Health Information to those companies. Neither Plaintiff nor Class Members ever gave Defendant permission to disclose their Personal Health Information to Facebook and Google.

381. Defendant also violated section 502, subsection (c)(1)(B), of CDAFA by knowingly accessing without permission Plaintiff's and Class Members' devices in order to wrongfully obtain and use their personal data, including their sensitive medical information, in violation of Plaintiff's and Class Members' reasonable expectations of privacy in their devices and data. Defendant achieved this by installing software code on its website that directed patients' browsers to send copies of their communications to Facebook and Google without their consent.

382. Defendant violated California Penal Code section 502, subsection (c)(2), by knowingly and without permission accessing, taking, copying, and making use of Plaintiff's and the Class Members' personally identifiable information, including their sensitive medical information as part of a scheme to barter patients' Personal Health Information to Facebook and Google in return for advertising benefits.

383. Defendant violated California Penal Code section 502, subsection (c)(6) by knowingly and without permission providing or assisting Facebook and Google with a means of accessing Plaintiff and Class Members' computer systems.

384. The computers and mobile devices that Plaintiff and Class Members used when accessing Defendant's website all have and operate "computer services" within the meaning of CDAFA. Defendant violated §§ 502(c)(3) and (7) of CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with Facebook's wrongful collection of such data.

385. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Defendant violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via Meta Pixel embedded into the hospital website which intercepted Plaintiff's and the Class Members' private and sensitive medical information.

386. Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

(a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

(b) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(c) Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(e) Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

387. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

388. Plaintiff and the Class Members seek compensatory damages in accordance with CAL. PENAL CODE § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable relief. Plaintiff continues to desire to search for health information on Defendant's website. She will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use Defendant's website to search for health information in the future.

389. Plaintiff and Class Members are entitled to punitive or exemplary damages pursuant to CAL. PENAL CODE § 502(e)(4) because Defendant's violations were willful and Defendant is guilty of oppression, fraud, or malice as defined in CAL. CIVIL CODE § 3294.

390. Plaintiff and the Class Members are also entitled to recover their reasonable attorney's fees under § 502(e)(2).

COUNT V—VIOLATION OF CAL. CIVIL CODE § 1798.82

391. Plaintiff re-alleges and incorporates all preceding paragraphs.

392. Plaintiff Jane Doe brings this claim on behalf of herself and all members of the Patient Subclass.

393. California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California … whose

unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

394. For purposes of the statute, "personal information" means "[a]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: … (D) Medical information." CAL. CIVIL CODE § 1798.82.

395. For purposes of the statute, "medical information" means "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."

396. Any customer who is injured by a violation of the statute may institute a civil action to recover damages. CAL. CIVIL CODE § 1798.84(b). Further, any business that violates, proposes to violate, or has violated this statute may be enjoined. CAL. CIV. CODE § 1798.84(e).

397. Defendant failed to disclose to Plaintiff and the Subclass that it was regularly collecting, transmitting, and sharing patients' unencrypted medical information with Facebook so that Facebook could target them with advertising. Along with its patients' medical information, Defendant also disclosed its patients' first names (or first initial and last name) to Facebook via encrypted data transmissions, including the unauthorized transmission of patients' Facebook IDs to Facebook, which permitted Facebook to link the medical information provided with the personal identities of Plaintiff and the Subclass Members.

398. Defendant willfully, intentionally, and/or recklessly failed to provide the disclosures required by California Civil Code section 1798.82 as part of a scheme to barter Plaintiff's and Subclass Members' Personal Health Information to Facebook in return for access to the Meta Pixel tool.

399. Plaintiff and Subclass Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Subclass Members under the guise of keeping this information private. Defendant collected, used, and

disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from Facebook and other third parties. Defendant had knowledge that Plaintiff and Subclass Members had conferred this benefit on Defendant by interacting with its website, and Defendant intentionally installed the Meta Pixel tool on its website to capture and monetize this benefit conferred by Plaintiff and Subclass Members.

400. Plaintiff and Subclass Members also conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiff's and Subclass Members' Personal Health Information. Defendant was aware of receiving these payments from Plaintiff and Subclass Members and demanded such payments as a condition of providing treatment.

401. Plaintiff and Subclass Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to Facebook. The services that Plaintiff and Subclass Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide.

402. The medical services that Defendant offers are available from many other health care systems who do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff's and Subclass Members' medical information without consent, neither Plaintiff, the Subclass Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

403. Defendant unjustly retained those benefits at the expense of Plaintiff and Subclass Members because Defendant's conduct damaged Plaintiff and Subclass Members, all without providing any commensurate compensation to Plaintiff and Subclass Members.

404. Plaintiff and Patient Subclass Members were damaged by Defendant's failure to inform them that their Personal Health Information was being shared with Facebook, resulting in, at minimum, the following damages:

(f) Sensitive and confidential information that Plaintiff and Patient Subclass Members intended to remain private is no longer private;

(g) Defendant eroded the essential confidential nature of the doctor-patient relationship;

(h) Defendant took something of value from Plaintiff and Patient Subclass Members and derived benefit therefrom without Plaintiff's and Patient Subclass Members' knowledge or informed consent and without sharing the benefit of such value;

(i) Plaintiff and Patient Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

(j) Defendant's actions diminished the value of Plaintiff and Patient Subclass Members' personal information.

405. Plaintiff also continues to desire to search for health information on Defendant's website. She will continue to suffer harm if Defendant does not make adequate disclosures regarding which third party marketing companies are receiving Plaintiff's and Patient Subclass Members' protected health information. Plaintiff and the Patient Subclass Members are therefore also entitled to injunctive relief requiring Defendant to comply with CAL. CIV. CODE § 1798.82.

COUNT VI – COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION

406. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth here and brings this claim individually and on behalf of the Santa Clara Valley Medical Center Class.

407. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its website and the communications platforms and services therein.

408. Plaintiff and Class Members communicated sensitive and protected medical information and personally identifiable information that they intended for only Defendant to receive and that they believed Defendant would keep private. Defendant installed source code on its website that surreptitiously instructed Plaintiff's and Class Members' browsers to share their Personal Health Information with Facebook, Google, and other third parties.

409. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

410. Plaintiff and Class Members had a reasonable expectation of privacy based on the sensitive nature of their communications. Plaintiff and Class Members have a general expectation that their communications regarding health and finances will be kept confidential. Defendant's disclosure of Private Information coupled with individually identifying information is highly offensive to the reasonable person.

411. Plaintiff and Class Members also had a reasonable expectation of privacy that their communications, identity, health information, and treatment data would remain confidential and that Defendant would not install surreptitious wiretapping technology on its website to secretly transmit their communications to third parties, including Facebook and Google.

412. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

413. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

414. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

415. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

416. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT VII – VIOLATION OF THE INFORMATION PRACTICES ACT CAL. CIVIL CODE § 1798.1, ET SEQ. (IPA)

417. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth here and brings this claim individually and on behalf of the Santa Clara Valley Medical Center Class.

418. Plaintiff and Class Members are "individuals" under Civil Code section 1798.3(d).

419. Defendant is an "agency" as defined under Civil Code section 1798.3(b).

420. The patient data collected and transmitted to third parties by Defendant constitutes "record(s)" and a "system of records" as those terms are defined by section 1798.3(g) and (h).

421. The personal health information and personally identifiable information disclosed by Defendant's unauthorized disclosures of Plaintiff's' and Class Members' data such as their names, addresses, telephone numbers, Facebook IDs, IP addresses, medical information, and other information constitutes "personal information" under section 1798.3(a) of the Civil Code. Defendant disclosed this personal information in violation of Civil Code section 1798.24 by failing to adequately secure and maintain it, thereby allowing unauthorized third parties to access and obtain it.

422. In violation of Civil Code section 1798.21, Defendant failed to establish appropriate and reasonable safeguards to ensure the security and confidentiality of Plaintiff's and

Class Members' personal information, and to protect against the unauthorized disclosure of such personal information.

423. On information and belief, Defendant violated Civil Code section 1798.19 by failing to cause contractors and subcontractors to abide by the requirements of the Information Act of 1977 when entering contracts for the operation and maintenance of records containing Plaintiff's and Class Members' personal information.

424. In violation of Civil Code section 1798.20, Defendant failed to establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing Plaintiff's and Class Members' personal information that effectively prohibited such persons from implementing technologies that would surreptitiously transmit patients' personal information to third parties like Facebook and Google.

425. In violation of Civil Code section 1798.24, Defendant knowingly disclosed Plaintiff's and Class Members' personal information in a manner that would link the disclosed information to Plaintiff and Class Members without disclosing the same to Plaintiff and Class Members and without securing the prior written voluntary consent of Plaintiff and Class Members.

426. In violation of Civil Code section 1798.29, Defendant unreasonably delayed in disclosing its unauthorized disclosure of its patients' personal information to Facebook and Google. Defendant was aware of the unauthorized disclosure of its patients' personal information as early as 2022, and certainly no later than June 2023, but declined to inform the public. There were no legitimate needs justifying the delay. Nor was the delay necessary to determine the scope of the breach and restore the reasonable integrity of Defendant's data system.

427. Civil Code section 1798.45 permits Plaintiff and Class Members to bring a civil action against Defendant for violating the IPA. Defendant's failure to adhere to the requirement of the IPA has adversely affected Plaintiff's and Class Members' interests, including by denying them an opportunity to take timely and appropriate protective measures in response to

Defendant's unauthorized disclosure of their personal information to Facebook and Google, such as choosing a different medical provider. In addition, as a result of Defendant's actions, Plaintiff and Class Members, have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being disclosed without authorization to Facebook, Google, and other third parties.

428. Accordingly, Plaintiff and Class Members are entitled to actual and statutory damages from Defendant under Civil Code sections 1795, 1798.48, and 1798.53 in an amount to be determined at trial, as well as injunctive relief pursuant to Civil Code section 1798.47, reasonable attorney's fees and costs, and any other relief deemed appropriate by the Court.

IX. DEMAND FOR JURY TRIAL

429. Plaintiff hereby demands a trial by jury on all issues so triable.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class and Subclass respectfully requests that the Court enter an order:

A. Certifying the Class and Subclass and appointing Plaintiff as the Class and Subclass representative;

B. Appointing the law firms of Ahmad, Zavitsanos, & Mensing PLLC and Caddell & Chapman as proposed interim class counsel;

C. Finding that Defendant's conduct was unlawful, as alleged herein;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. Awarding Plaintiff and the Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiff and the Class Members pre-judgment and post-judgment interest;

G. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

Dated: August 25, 2023

Respectfully submitted,

By: */s/ Michael A. Caddell*

Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
628 East 9th Street
Houston TX 77007-1722
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson (SBN 289055)
Joseph Ahmad*
Nathan Campbell*
Ahmad, Zavitsanos, & Mensing, PLLC
1221 McKinney Street, Suite 2500
Houston TX 77010
(713) 655-1101
fjohnson@azalaw.com
jahmad@azalaw.com
ncampbell@azalaw.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

* Motions for Admission to be filed

COUNSEL FOR PLAINTIFF, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED